

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED

FEB - 2 1995

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF SECRETARY

In the Matter of)

)

)

CC Docket No. 92-115

Revision of Part 22 of the)
Commission's Rules Governing)
the Public Mobile Services)

DOCKET FILE COPY ORIGINAL

REPLY TO COMMENTS OF MCCAW CELLULAR
COMMUNICATIONS, INC. ON PETITIONS FOR RECONSIDERATION

C-Two-Plus Technology, Inc. ("C2+") replies to the "Comments of McCaw Cellular Communications, Inc. on Petitions for Reconsideration and Clarification" ("McCaw Comments") in this proceeding. Ironically, McCaw attempts to portray C2+ cellular "extension" phone service as a "'rip-off' [of] cellular carriers and their subscribers" (McCaw Comments at 5) at the same time that it and other cellular carriers are deploying their "extension" cellular services in a manner which will cost cellular consumers billions of dollars in unnecessary monthly recurring service charges. Because C2+ offers a far more economical alternative to cellular consumers desiring "extension" phone service, McCaw and other cellular carriers continue to attempt to drive C2+ from the marketplace by alleging, without foundation, that C2+ contributes to cellular fraud.

No. of Copies rec'd CH 11
List ABCDE

Preliminary Statement

McCaw claims that it opposes the C2+ cellular extension phone service because the C2+ service "will only increase the fraudulent usage already present in the cellular industry." McCaw Comments at 14. Thus, McCaw denies that its opposition to the C2+ service is "being motivated only by greed" or a desire "to stifle competition," claiming that "[t]o suggest that cellular carriers -- many still seeking to establish themselves competitively and financially -- would deny customers a service they want is patently absurd." Id. at 5, 11. C2+ respectfully submits that it is anything but "absurd" to suggest that the carriers have designed their cellular extension service offerings to maximize their stream of monthly recurring revenues and have sought to "stifle competition" from entities like C2+ which offer a far more economical alternative to cellular consumers. That is precisely what the carriers are doing to C2+ under the guise of implementing "anti-fraud measures" in this proceeding.

I. C2+ Does Not Contribute To Cellular Fraud

Undeterred by the absence of any evidence that C2+ phones have been used fraudulently,¹ McCaw analogizes the C2+

¹ In its Petition for Reconsideration, C2+ stated that "it has not learned of a single instance in which one of its customers has engaged in fraudulent use of cellular service and no cellular carrier has ever advised C2+ that a phone programmed by C2+ has been used fraudulently." C2+ Petition for Reconsideration in CC Docket No. 92-115, filed Dec. 19, 1994 ("C2+ Petition"), at 8. Apparently, the carriers are

service to satellite signal piracy and cable theft, claiming that it is "just another subset" of activities "intended to 'rip-off' cellular carriers and their subscribers" by enabling "individuals to obtain substandard services without paying for them." McCaw Comments at 5. Of course, McCaw simply ignores the fact that -- in contrast to satellite signal and cable pirates who steal those services without paying for them -- the very reason that a cellular subscriber authorizes C2+ to emulate the ESN of his primary cellular phone is so that the subscriber will be billed and pay for calls made from the additional phone.² Conceding that it has no evidence that any

equally unaware of any such fraudulent use because in response to the C2+ Petition, they have not identified a single instance of fraud attributable to a C2+ customer. See McCaw Comments at 9.

² The primary function of the electronic serial number ("ESN") of a cellular phone is to "enable the carriers to bill properly for calls made from the telephone." Report and Order, CC Docket No. 92-115, 9 FCC Rcd. 6513 (1994) ("Report and Order"), at ¶54. Replicating the ESN of a paying cellular customer without the customer's authorization in order to make calls which are billed to the unsuspecting customer is known as "cloning" fraud. See McCaw Comments in CC Docket No. 93-292, filed Jan. 14, 1994, at 4; Notice of Proposed Rulemaking, CC Docket No. 93-292, 8 FCC Rcd. 8618 (1993), at ¶33. Continually changing ESNs to make calls which the cellular carrier is unable to bill is known as "tumbling" fraud. Id. In contrast to such activities, C2+ replicates the ESN of a paying cellular subscriber at the subscriber's request to enable the customer to make and pay for calls from an additional phone which is either a replacement for, or "extension" of, the customer's primary cellular phone. See Affidavit of Stuart F. Graydon attached as Appendix 1 ("Graydon Aff.") at 1-2 and Exhibit 1. Such service does not involve "cloning," "tumbling" or any other kind of fraud.

C2+ customer has engaged in cellular fraud,³ McCaw claims that "[t]he absence of fraud evidence...is merely a red herring" (McCaw Comments at 9) and attempts to manufacture a possible scenario, no matter how remote and speculative, in which C2+ service might be used fraudulently.

First, McCaw contends that "cellular carriers routinely terminate service to cellular numbers when the same ESN/MIN registers on the system in more than one location," and conjectures that "[s]ome percentage" of such terminations "are undoubtedly due to the activities of C2+ and its customers." McCaw Comments at 9. However, neither McCaw nor any other cellular carrier has identified a single C2+ customer so terminated, and C2+ has never been informed by any customer that a carrier has terminated his service due to use of a C2+ extension phone. See Affidavit of Carol Patton, attached as Appendix 1 to C2+'s "Reply to Cellular Telecommunications Industry Association Opposition to Petition for Reconsideration," filed Feb. 2, 1995 ("Patton Aff.") at ¶10.

Next, McCaw speculates that C2+ might be tricked into performing its service for someone who is not a bona fide cellular subscriber because "false identification can readily be obtained and presented." McCaw Comments at 9. However,

³ Although the carriers repeatedly have claimed that "anyone" can use a C2+ device to reprogram an ESN, that statement is simply false because the device will not reprogram a phone without specific authorization codes provided by C2+. See Graydon Aff. at 1-4 and Exhibits 2-3; C2+ Petition at 8-11 and Exhibit 1.

McCaw concedes that C2+ requires its dealers to obtain "photo identification" to ensure that the customer is who he says he is. Id. McCaw also concedes that C2+ "requires its customers to prepare an application containing name, address [and] land-line telephone number" of each customer, as well as documentation that the customer is "an authorized cellular subscriber." Id. Although McCaw characterizes these precautions as "worthless" (id.), the carriers have not identified a single instance in which C2+ service has been used fraudulently, either through "subscription" fraud or "cloning," and C2+ has no knowledge of any such fraudulent use. See Graydon Aff. at 1; see also C2+ Petition, Exhibit 1 at ¶11. Of course, additional protection against subscription fraud could be provided by contacting the prospective customer's carrier if the carriers would cooperate with C2+, but thus far carriers have been unwilling to do so.

McCaw then claims that C2+ "has no way of knowing whether the customer is in good standing with the cellular carrier." McCaw Comments at 9-10. Again, if the carriers would cooperate, C2+ could confirm the customer's status directly with the carrier before servicing that customer. See C2+ Petition at 22-23. Absent such cooperation by the carriers, C2+ ensures that the customer is in good standing by requiring a copy of a recent bill from the customer's carrier (id. at 9), and even McCaw concedes that "C2+ requires a

potential customer to provide evidence that it is an existing subscriber to cellular service." McCaw Comments at 13 n.14.

In short, McCaw has provided no evidence of fraudulent use of C2+ services and its feeble attempts to manufacture the possibility of such fraudulent use are contradicted by the undisputed fact that C2+ provides its emulation services only for bona fide cellular subscribers desiring either to replace a damaged cellular phone or to obtain cellular "extension" service.

II. C2+ Does Not Impair System Operations Or Fraud Detection Procedures

Unable to generate any evidence that C2+ facilitates cellular fraud, McCaw contends that "the legitimacy or illegitimacy of C2+'s intent in developing and marketing its service does not matter" -- and the fact that C2+ provides the service only to "legitimate cellular customers is entirely irrelevant" -- because the "integrity of the system itself is undermined" by the C2+ service. McCaw Comments at 8. Other than its repeated incantations of the importance of "system integrity" and speculation regarding future "fraud attacks" and "advanced anti-fraud programs," McCaw offers nothing to support its claims -- which plainly are contradicted by the fact that C2+ phones have been operating on cellular systems across the country for three years without incident. See Patton Aff. at ¶10; see also Graydon Aff. at 1.

For example, McCaw contends that "a C2+ emulated phone degrades the level of service provided by carriers" because "[n]otwithstanding C2+'s direction to users that the multiple phones cannot be simultaneously operated, many subscribers in fact will have all phones turned on." McCaw Comments at 12-13. However, the "two phones/one number" and other similar extension phone services being deployed by the cellular carriers require similar warnings to the customer that "only one phone can be turned on at any one time." See C2+ Petition at Exhibit 2 (marketing materials for carriers' "Flexphone" and "2 Phones/1 Number" services). McCaw never explains why: (a) the carrier's customers are better able to follow these instructions than the C2+ customers, particularly since the C2+ customers are the carrier's customers; and (b) the level of service degrades when multiple C2+ phones are on contrary to C2+ instructions, but not when multiple carrier phones are on contrary to the carrier's instructions.

McCaw also finds fault with C2+'s proposal to provide cellular carriers with a list of C2+ customers to assist in their fraud detection procedures while preserving the consumer benefits inherent in the C2+ "extension" phone service. First, McCaw speculates that because the list "is dependent on the quality of the information given to C2+...[it] may contain fraudulent users." McCaw Comments at 10. If such fraudulent users existed (and C2+ has never been informed that any customer has used its services fraudulently), McCaw does not

explain why a cross-check of the C2+ and the carrier's customer lists would not expose them. McCaw also claims that if a thief cloned a C2+ customer's ESN, the "cloned phone...would 'hide' behind the emulated phone, with the C2+ list assisting in that process" by granting the user "further protection from detection." Id. at 10-11. However, the C2+ customer list offers no such "further protection" because in addition to knowing the identity of the customer, the carrier would know how many extension phones the customer is using. Consequently, if the carrier's C2+ customer list indicated that a particular customer had one C2+ extension phone, detection of "the same ESN/MIN combination" on the system at more than two locations would indicate fraud, prompting inquiries to the customer. Id. at 9.⁴ Moreover, the Personal Identification Number ("PIN") services being rolled out by the carriers provide additional fraud protection by using the PIN (which the customer can change at will) as an additional authentication method. Thus, fraudulent users would receive no "further

⁴ However, it is far more likely that other detection procedures (i.e. detection of aberrant calling patterns) would indicate fraudulent use much sooner. For example, fraudulent use of cellular service often involves long-distance calls, and long-distance carriers notify cellular carriers "of possible fraudulent activity when they have noticed spikes in international calling or long-distance calling" on customers' cellular phones. See McCaw Reply Comments in CC Docket No. 93-292, filed Feb. 10, 1994, at 7.

protection from detection" if the carriers maintained a C2+ customer list.⁵

Finally, without providing any empirical data, McCaw contends that "each cellular telephone operating on a system imposes other costs" in addition to a "usage cost," even when the subscriber "is not actually using the phone to place and complete calls." Id. at 12. C2+ respectfully suggests, however, that such incremental costs are de minimis and cannot justify the recurring monthly service charges of \$20 to \$40 currently imposed by the carriers for cellular extension service. See C2+ Petition at 13 n.8 ("The consumer would be substantially better off paying...a nominal charge" to cover the carrier's incremental costs to implement C2+ extension service rather than paying the "monthly subscription charges currently required by the carriers."). In fact, based on estimates of demand for cellular extension phone services over the next five years, the potential savings to cellular customers through use of the C2+ technology amounts to billions of dollars. See Graydon Aff. at 4-5 and Exhibit 4; see also Petition for Reconsideration of MTC Communications in CC

⁵ McCaw also contends that C2+ technology "is incompatible with advanced anti-fraud programs such as RF 'fingerprinting'." McCaw Comments at 7. However, McCaw never claims that such "fingerprinting" programs are being used or will be used in the foreseeable future. Likewise, McCaw never explains why the C2+ technology is necessarily incompatible with those programs. For example, McCaw never explains why one cellular subscriber could not have multiple RF "fingerprints."


Docket No. 92-115, filed Dec. 19, 1994, at 11. Under those circumstances, it certainly is not "patently absurd" to suggest that the carriers might attempt to stifle competition for their "extension" phone services. See Graydon Aff. at 3-6; Patton Aff. at ¶14 and Exhibit F.

Conclusion

McCaw's efforts to prohibit use of the C2+ technology are not based on concerns over cellular fraud or the integrity of the cellular system, but rather on McCaw's desire to preserve a substantial recurring monthly revenue stream from its own "extension" phone services. Absent any evidence supporting McCaw's allegation that the C2+ services "will only increase the fraudulent usage already present in the cellular industry," the Commission should not permit the carriers to prohibit C2+ extension service under the guise of implementing anti-fraud measures.

February 2, 1995

Respectfully submitted,



Timothy J. Fitzgibbon
Thomas F. Bardo
Carter, Ledyard & Milburn
1350 I Street, N.W., Suite 870
Washington, D.C. 20005

Attorneys for
C-Two-Plus Technology, Inc.

Appendix 1

AFFIDAVIT

BEFORE ME, the undersigned authority, personally appeared Stuart F. Graydon, who, having been duly sworn by me, deposes on oath and says as follows:

"I, Stuart F. Graydon, a resident of the State of Florida and Executive Officer of C2+ Technology, Inc. (hereinafter C2+), duly incorporated under the laws of the State of Alabama, do hereby voluntarily make the following statements:

Beginning in 1989, I became involved in the development of technology to enable a legitimate subscriber of cellular services to add extension phones to their existing line for which the subscriber is paying the required monthly line fee (for his number) plus the carrier specified per minute usage charge for each system access.

As the technology was being developed, we took special precautions to insure that all calls made by either phone were billed, the result being that regardless of which phone was used, the carriers would receive the same revenues as if each call were made by the same phone, thus there would be no additional costs to the carrier to allow this service and the carrier would immediately benefit from increased airtime usage.

After completing and field testing this technology on numerous carrier switches and software (some tests being conducted by C2+ and others by Carriers and/or their Agents), there was NO instance reported where a call was made that was not billed. At first, all phones were emulated at our facility. We ran the first ad the last week of January, 1992 and received over 600 calls from this ad alone! Responding were individuals, cellular dealers, repair centers, agents, and carriers, many of them McCaw related companies and agents. All of them expressed a

desire to have this feature which many stated that the carriers had been denying them this service by saying that it was technically impossible.

Next our technicians perfected a process whereby a dealer could perform the emulation on site rather than send phones to us and have the customer wait a week to get the phone back. To improve identification and verification of the customer as a legitimate subscriber in good standing, they were required to provide a copy of their current cellular bill, their Social Security Number and driver's license with a picture to compare.

The final security was to provide an encrypted method of authorizing the emulation. An NEPD Device was developed which would decrypt the code and allow only one emulation to be provided per code. Not only would this prevent unauthorized persons from using the Device but, should attempts be made to access the Device with an unauthorized number, the phone would be rendered inoperative, requiring it to be returned to the factory for servicing. An overview of this Device is attached as Exhibit 1. Since three of the five groups of information required for a code remained in the C2+ mainframe computer, the necessary information to calculate and decrypt the code is never made available to the user.

This NASA type DES (Digital Encryption System) has many levels of encryption, using at least five separate eight to eleven digit numbers, manipulating them in a way that they cannot be reverse engineered mathematically.

On several occasions we called the FCC and spoke with various members of the Mobile Services Division. We were referred to Eric Hill at CTIA and he told me that there was a great need in the industry for this feature but that CTIA thought that only the carriers should provide it. At no time we were informed that what we were developing was illegal

or that it was not in the best interests of the public.

In September, 1992, I received a call from Eric Hill, Director of Security for CTIA. Mr. Hill said that sixteen of his carriers were interested in our technology and that he had been asked to contact us for further information. He said that there was a definite need for the consumer to have this product but he could not evaluate it without some type of testing. I asked him which carriers had requested this and he specifically named McCaw, Contel, GTE, Bell, US West, Nynex, Cellular One, Pactel, and Palmer Communications. Upon written request (Exhibit 2) C2+ sent CTIA a NEPD Device to assure them that it could not be used randomly or by unauthorized persons to change an ESN for any reason - fraudulent OR non-fraudulent. CTIA was unable to use it without the specific C2+ codes.

In CTIA's month-long testing they first attempted to access the phone without C2+ supplied codes and locked up the phone (as the Device security was designed to do), requiring the factory to restore it to operation. Next, he submitted a proper request for the codes for a specific pair of phones. C2+ then supplied the proper codes. CTIA successfully emulated that phone, but when they again tried to enter an unauthorized code, the phone again locked up. At this point, CTIA took the phone and Device to a meeting at the FCC and told them that CTIA had used a C2+ Device to alter a phone and that ANYONE could use the C2+ Device to alter a phone for the purpose of committing fraud.

In 1992, I spoke with Mr. Nelson Roberts, Vice President of Telephone Warehouse in Dallas whose company is the largest of its kind in Dallas and he advised me that they activated over 10,000 phones per month nationwide.

We spoke several times over the next few months and he assured me that if his carrier, METROCEL (a McCaw company), would approve it, that he

would be the largest Distributor for C2+ in the country.

Subsequently C2+ provided samples for Mr. Lee Maschmann, Metrocel's Chief Engineer and coordinated testing with him. Mr. Maschmann found no problems with the operations or negative effects on the system and Mr. Roberts pursued it with local management. When local management requested approval from McCaw's main office, they were flatly refused. Mr. Roberts was "reminded" that Metrocel could cancel his Contract at any time or fail to renew it. Mr. Roberts then advised me that "his hands were tied because Metrocel was the primary source of their income."

The next year I flew to Dallas and had lunch with Mr. Roberts. In the presence of a NovAtel employee Mr. Roberts stated that Metrocel "reminded" him that if they terminated his Contract that Telephone Warehouse would lose over \$1,500,000 a year in residuals. Mr. Roberts stated that they could not afford to alienate them regardless of the additional sales and customers he could generate by doing business with C2+. McCaw told them that they would be able to offer a similar service by Fall of 1993. To date, McCaw is not offering this service in the Dallas area nor in any other area that I am aware.

In retaliation for their agents referring customers to C2+, McCaw has issued bulletins misquoting the new FCC rules and announcing that they will be withholding from their agents' commissions and residuals \$1,000.00 for EACH LINE which has a C2+ extension phone! (Exhibit 3)

I understand that McCaw franchises cover 1/3 of the entire population of the United States. Thus far, the public in the approximately 150 areas served by McCaw have been denied this service. I believe that if McCaw is allowed to put C2+ and other small businesses using its proven fraudproof encrypted C2+ Technology out of business, then the public is

being deprived of BILLIONS of dollars without justification based on the attached calculations. If the public is ALLOWED to have their legal rights to extension phones provided by independent third parties, then the consumers could save over an estimated FIFTEEN BILLION Dollars over the next five years !! (See Exhibit 4).

No evidence has been presented to justify the totally unfounded allegation that "C2+ 'type' technology has been used to alter phones for the purpose of defrauding legitimate subscribers or that it has been used by those engaged in illegal narcotic activities. As C2+ deals only with a carrier's legitimate cellular subscribers, C2+ would be involved in such activities only to the extent of that of the carriers' customers use their phones for such odious and reprehensible activities? .

I believe that one factor that the carriers want to hide is the fact that the market value of their franchise is based not on their net revenues but on the number of subscribers. I understand their subscriber contracts state that each NUMBER is a SEPARATE customer, regardless if it is the same person. Consequently, a carrier will give away a phone that costs them \$300.00 and pay up to \$400.00 in activation commissions plus up to 15% residuals to gain another subscriber although the revenues from that 'sale' may take the carrier up to two years to recover.

Report and Order 92-115, paragraph 22.919 refers to FRAUDULENT manipulation of the ESN. C2+ does NOT alter the ESN for fraudulent purposes. C2+ ONLY alters the ESN on behalf of a legitimate subscriber in good standing who owns both phones and only wants an extension on the one line for which they are paying. Both C2+ and the consumer do not believe this to be fraudulent.

In a recent memo which I have received (see Exhibit 3), McCaw boasts that:

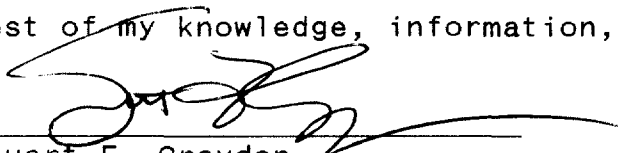
"WE have also CONVINCED the FCC to prohibit the use of all ESN emulation devices (such as those sold by a company called C2+) EVEN IF the users claim they are merely duplicating THEIR OWN PHONE in order to have "two phones, one number" capability. Persons violating this rule are subject to strict fines."

The news media recently quoted FCC Chairman Reid Hundt as stating:

"I'm always asked to boil (the FCC's) philosophy down to one word, and that's competition...I can't tell you how often I have heard that communications is for the big guys. I am not against the big companies, but I am against the view that only they can participate in wireless opportunities."

If one small company like C2+ is not free to engage in its legitimate business activities and compete with the big guys, then none of us are free and we do not truly live in a free country where all people are equal in the eyes of the law."

The statements made in this affidavit are true and correct to the best of my knowledge, information, and belief.


Stuart F. Graydon

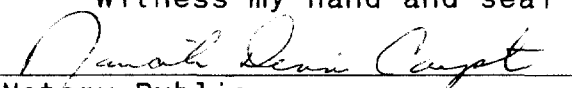
1-30-95
Date

STATE OF ALABAMA }

COUNTY OF MONTGOMERY }

I, the undersigned authority, a Notary Public, in and for said County in said State, hereby certify that STUART F. GRAYDON, whose name is signed to the foregoing instrument, and who is known to me, acknowledged before me this day that, being informed of the contents of such instrument and with full authority, executed the same voluntarily on the day the same bears date.

Witness my hand and seal this the 30th day of January, 1995.


Notary Public

My Commission expires 6/2/96

Exhibit 1

C-TWO-PLUS-TECHNOLOGY

3174 Mobile Highway - Montgomery, AL 36108 - Phone [205] 264-0264 - FAX 264-7190

C TWO PLUS TECHNOLOGY NEPD-100 DEVICES

Each C TWO PLUS NEPD Device is an individually customized microelectronic device designed primarily and specifically for the transfer of ESNs from one phone to another.

While other manufacturers may allow ESN transfers to be done through a simple cable and plug assembly with materials readily available from Radio Shack, they do not track these ESN changes. C2+ technology cannot be used without first submitting specific information and then obtaining special decryption codes, all of which are data based by C2+ to identify possible fraud. The C2+ technology and its Devices are not intended for or represented to be used for theft of services or any illegal purposes.

APPLICATIONS:

(1) During repairs and to prevent added cost, delay and the inconvenience of changing the customer's ESN at the switching office or other locations which is an accepted procedure by several major manufacturers and is currently and routinely being performed by carriers and their agents.

(2) Multiple phones on one number where applicable and allowed.

There may be other applications and consumer benefits which do not relate to fraudulent use which may be in the best interests of the consumer.

This Device is the result of over two years of development and engineering and represents the most secure factory level state-of-the-art methods of transferring the ESN available today. Unlike 'chipping' (which may be illegal) the manufacturer's copyrighted software is not altered nor are physical components added which might violate original FCC Type Approval.

As C TWO PLUS TECHNOLOGY is vitally concerned with the prevention of theft of services and cellular fraud, only a small part of the required programming is in either the firmware chips or the Device - the balance being contained in the C TWO PLUS TECHNOLOGY Mainframe Computer in its main office. C TWO PLUS employs sophisticated NASA type DES encryption algorithms to protect the integrity of the software and to prevent unauthorized emulations which might be used for illegal purposes.

For this reason C TWO PLUS NEPD Devices are not sold but are available to qualified Distributors and Dealers ONLY on a special limited Lease basis.

Contrary to equipment manufacturer's field instructions which are not monitored or controlled, C TWO PLUS requires that the Device Lessee submit to C TWO PLUS specific information and verification of authority of the end user each time a transfer (emulation) with the Device is performed and a charge is made for each set of code numbers supplied. This information is stored into the C TWO PLUS master database for billing and to be available for inspection by authorized parties.

At the time C TWO PLUS issues the upload codes the Lessee may request and receive the download codes to restore the phone to its original ESN. The C2+ supplied codes DO NOT allow transfer of ANY OTHER ESN's without additional code requests.

C TWO PLUS NEPD DEVICES:

The NEPD-100 Series Device is a self-contained micro-miniature decryption computer designed to be used in the field. This Device utilizes the phone's power source, keypad, and display for operator I/O and special plug-in copyrighted firmware for transfer programs. Communications at bus level architecture and I/O through a special interconnect cable are achieved using a standard connector found in each transceiver.

The C TWO PLUS firmware is different for each manufacturer's model phones and cabling may also vary from manufacturer to manufacturer. Software for these Devices is constantly being upgraded and additional models for ESN transfer added upon completion of field testing. Although transferring the ESN with the NEPD Device is relatively simple, calculating the information required to transfer an ESN by the C2+ method is extremely complicated making it the most secure method in the industry.

In order for a transfer to take place ALL keys must match precisely. The first two keys are the 11 digit ESNs of the two phones. This information is readily available to the user and is all that is required to perform other manufacturers' and carriers' transfer procedures. C2+ procedures, however, require THREE ADDITIONAL keys which are NEVER accessible to others. The third C2+ key is an 16 bit encrypted number that is unique to that Device. The fourth key is another 16 bit encrypted number that is stored in the C2+ Master Computer, is unique to each Device Lessee, and is known only by one person at C2+. The last key is only known by the C2+ encryption software writers and determines the algorithms and permutations required to produce the transfer number. The odds of anyone randomly developing a decryption is 2^{64} .

Further, should an attempt be made to enter more than a preset number of unsuccessful 'trials', the Device will shut off and the phone becomes inoperative (as FCC/EIA specifications indicate it should) and the phone must be sent to C TWO PLUS to be restored. This is an additional C2+ fraud detection feature and to date no one has been reported as successfully circumventing the NEPD Device's decryption system. Whereas other procedures involving "chipping" or "cloning" may hinder attempts to circumvent fraud, C TWO PLUS TECHNOLOGY monitoring assists in detecting such practices.

For phones in which the ESN's are not easily transferred because of special cable and fixture requirements, at the specific request of and as an agent for the authorized subscriber and after receiving proper proof of ownership and authority, C TWO PLUS may provide emulations in its Lab.. C TWO PLUS TECHNOLOGY does not make any warranties or assume any liability or responsibility for any use or non-use of its products except as may be individually and specifically contracted between such individual parties in writing and executed by its duly authorized corporate officers.

Contact Ms Carol A. Patton at [205] 264-0264 for further details.

COMPARISON OF C2+ and CARRIER METHODS

There are two legitimate ways to provide cellular extensions. The carrier methods, which are more expensive and require continuing monthly charges, and the new C2+ TECHNOLOGY which is more flexible, practical, and economical.

CARRIERS:

1. Usage LIMITED to Carrier's local area.
2. Activation charges PLUS continuing monthly charges for 2nd line.
3. Second phone CANNOT Roam.
4. Only ONE phone powered ON at a time.
5. Monthly charges and fees may increase
6. Designed to sell MORE LINES and monthly charges rather than selling airtime use.
7. Only two phones may be on the system.

C2+ TECHNOLOGY:

- Works on ALL SYSTEMS WORLDWIDE !
- Only a ONE-TIME Emulation charge. NO second line or monthly charges.
- EITHER phone may Roam.
- SAME (Due to Cellular SYSTEM design)
- NO additional charges.
- Designed for convenience and security at an affordable price
- MULTIPLE phones may have SAME Number.

In addition, C2+ Emulated phones may be reset back to their original parameters if the other phone is stolen or the customer decides to sell the secondary phone.

C2+ - THE LOGICAL ALTERNATIVE

The only other secure method of having multiple cellular phones on the same number is the copyrighted C2+ NASA type DES Encrypted Emulation Technology. C2+ allows your cellular phone to maintain its original security, does not alter the manufacturer's software, physically add anything to the unit, nor does it violate the phone's original FCC type approval or system compatibility.

Phones with C2+ Emulations are not limited to specific areas or carriers but can operate ANYWHERE IN THE WORLD! There is only a one-time charge for the C2+ Emulation. Since you only use one line, there is no additional line charge to pay and only one phone may be powered on at a time.

SECURITY WITH C2+

While fly-by-night 'cloners, chippers' and Satellite pirates may alter phones to steal services, C2+ Emulation, developed by C2+ in 1989, assures the confidentiality and security of your information. C2+ maintains ONE on ONE customer support, providing updated information to subscribers and dealers.

To further insure the protection of the current cellular systems due to their deficiencies, phones with C2+ installed are transparent to the system, neither disrupting billing systems, circumventing fraud detection programs, nor violating carrier tariffs. All calls made on C2+ emulated phones are billed, assuring carriers of all airtime revenues.

Exhibit 2



September 25, 1992

Mr. Rick Graden
Chief Engineer
Cellular Two Plus
3174 Mobile Highway
Montgomery, AL 36108

Dear Mr. Graden:

Thank you for the opportunity to discuss with you today the C2+ technology. I appreciate your cooperation with sharing details of how the NAM Emulation Programming Device operates. I look forward to receiving the unit for purposes of reviewing with CTIA's technical staff.

As I stated, CTIA is very concerned with any device that may be used to commit fraud. Examination of the NEPD will provide us with a better explanation of how the system operates, and whether it poses a fraud issue.

We are also concerned with industry compliance with the Federal Communications Commission rules on ESN security. As I more closely examine the C2+ procedure for overwriting the existing ESN with the duplicate ESN, I will share my thoughts with you.

CTIA's examination of C2+ is solely for the purpose of furthering our understanding of how your product relates to individuals using it for fraud. Our review is not an endorsement of your product.

As our study progresses, I will contact you. If you have any questions, please do not hesitate to contact me at (202) 785-0081.

Yours Sincerely,

Eric Hill
Director of Industry Security

(MICHELLE SULLIVAN)

Cellular Telecommunications Industry Association

1133 21st St. N.W., Third Floor, Washington, D.C. 20036 • (202) 785-0081 • FAX (202) 785-0721



recycled paper

As our study progresses, I will contact you. If you have any questions, please do not hesitate to contact me at (202) 785-0081.

C-TWO-PLUS-TECHNOLOGY

3174 Mobile Highway - Montgomery, AL 36108 - Phone [205] 264-0264 - FAX 264-7190

EMULATION ORDER FORM

FAX# or phone: 1-800-723-5366

SECONDARY PHONE:

TYPE OF PHONE (MAKE/MODEL)

Audiovox CMT-420

VERSION OF FIRMWARE

M1-2

DEALER CODE (3 DIGIT) #

142

MASTER/PRIMARY ESN

13500871458

SLAVE/SECONDARY ESN

13801634822

ORDER PLACED BY

Eric Hill

FOR (CUSTOMER NAME)

Eric Hill, C.T.I.A

DEALER FAX # FOR RETURN
CODE

202-785-4090

SPECIAL INSTRUCTIONS:

DATE REQUESTED/TIME 10/20 - 3:45pm

DATE REQUIRED/TIME 10/20 by 5pm

CARRIER Cellular One

CITY/ST Washington/Baltimore

FOR C2+ OFFICIAL USE ONLY:

Code Rec'd by: _____

Date/Time _____

3 copies - Distribute to: Accounting/Marketing/Technical

Load Calculated by: _____

Date/Time Returned _____

